BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND

AIR FORCE INSTRUCTION 33-129

AIR FORCE MATERIEL COMMAND Supplement 1

28 JANUARY 1999

Communications and Information

TRANSMISSION OF INFORMATION VIA THE INTERNET

NOTICE: This publication is available digitally on the HQ AFMC WWW site at: http://afmc.wpafb.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFMC/SCDP (MSgt Wayne Allen)
Supersedes AFMCPD 37-1, 19 Feb 96; AFMCI 37-102, 15 Mar 96.

Certified by: HQ AFMC/SCD (Mr Gary Brooks)
Pages: 6
Distribution: F

This supplement applies to all Air Force military and civilian personnel, including Air National Guard or US Air Force Reserve (AFRES) and their use of public internet and web technology such as web servers, web browsers, and file transfer protocol (FTP) software purchased and licensed by the United States Air Force (USAF), or privately licensed software used with proper approval on USAF-owned systems. Units may further supplement this air force iinstructionI and command supplement, as required. Field units will send copies of supplements to HQ AFMC/SCDP, 4225 Logistics Avenue, Suite 6, Wright-Patterson AFB OH 45433-5745.

SUMMARY OF REVISIONS

This revision added several new areas such as new policy regarding World Wide Web (WWW) server administration and support, indexing, WWW page organization and maintenance, and information review and release. It also adds responsibility for recurring training for offices of primary responsibilities OPR) and page maintainers to the communications systems security officers' (CSSO) initial and annual training requirement. A checklist for OPRs and page maintainers for use before posting information to the internet has also been added. Warner Amendment provisions for transmitting sensitive unclassified information and a mandate to disconnect systems not authorized or accredited by the designated approving authority (DAA) are also included in this revision.

AFI 33-129, 1 January 1997, is supplemented as follows:

3.9.1. (Added) CSSOs are additionally responsible for, as part of the initial and annual training requirement, ensuring OPRs and page maintainers are educated on their roles and responsibilities. CSSOs will also ensure all users are educated on Air Force, command and local policies regarding official and authorized Internet use.

3.12. (Added) AFMC Information Assurance Office. Assess WWW server and bulletin board systems for authorization compliance as an item of interest during MAJCOM Information Assurance assessments.

4.1.2. (Added) Core Webmaster Requirements. The commitment to a WWW site should not be taken lightly by an organization. Web sites are not only key components of communications infrastructure but also project the organization's image. To ensure quality communications capabilities and maintain the best possible image, core requirements to support web sites have been identified. Organizations who do not meet these requirements for support of their web server(s) are not permitted to operate a web server and are required to host their information on a web server which meets the support requirements. The following skills are required for a webmaster contingent (1 or more individuals) to administer a WW server.

4.1.2.1. (Added) Certified Systems Administrator Training. Training requirement for webmasters based on the platform and software used to operate the specific WWW server being administered. Training is commonly available from the specific platform or software vendor and should include background in system security and other networking functions associated with the server to be administered.

4.1.2.2. (Added) Hypertext Markup Language (HTML). Training requirement for webmasters in order to develop host server's top level pages and to assist page maintainers who will maintain lower level web sites.

4.1.2.3. (Added) Graphics Format and Conversion. Quality graphics and presentation are essential in web development. Webmasters are required to have this training in order to develop host server's top-level pages and to assist page maintainers who will maintain lower level web sites.

4.1.2.4. (Added) Indexing. Each AFMC web server is required to have a searchable index for its information. This index will be consistent with the information's various access and security controls. It is essential webmasters be proficient in server indexing software and indexing techniques. Webmaster(s) of the HQ AFMC web server will be required to maintain a metaindex (index of indexes) of all information within the command's web.

4.1.2.5. (Added) Quality Performance Indicators (QPI). Webmasters are required to be proficient in employing tools to provide adequate performance statistics (server usage, page accesses, etc.) for their customers.

4.1.3. (Added) Recommended Webmaster Requirements. In addition to the core webmaster requirements, it is strongly recommended webmasters have an adequate background in programming/scripting (Perl, etc.), database interfacing, and multimedia authoring. The future of the web and internet will involve interfacing legacy systems with web pages.

7.2.1.3. (Added) Public Access Clearance Checklist. In addition to the tables provided in AFI 33-129, HQ AFMC/PA has developed a checklist (Attachment 2 (Added)) to assist OPRs in preparing information for posting in a publicly accessible area.

7.4.9. (Added) Sensitive But Unclassified (SBU) information subject to provisions of Public Law 100-235, The Computer Security Act of 1987, Section 2315 of Title 10, United States Code, The Warner Amendment. Such information is referred to as "national security information." National security information cannot be transmitted across the nonsecure internet unless it uses an encryption technology approved by the National Security Agency (NSA). (NOTE: As of this writing, no such encryption technology has yet been approved by NSA.) National security information is information which:

7.4.9.1. (Added) Involves intelligence activities.

7.4.9.2. (Added) Involves cryptologic activities related to national security.

7.4.9.3. (Added) Involves the command and control of military forces.

7.4.9.4. (Added) Involves equipment that is an integral part of a weapon or weapons system; or

7.4.9.5. (Added) Is critical to the direct fulfillment of military or intelligence missions--this does not include acquisition of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

7.4.9.6. (Added) All other SBU information. Information which does not qualify as national security information (for example, some types of Privacy Act and FOUO information) must be encrypted using an encryption technology approved by the National Institute of Standards and Technology (NIST), and comply with Federal Information Processing Standard (FIPS) 140-1. A list of approved encryption technologies is available from NIST. At the time of this writing, the list was available on the web at http://csrc.ncsl.nist.gov/cryptval/140-1/1401val.htm.

7.5. Internet release packages are subject to review during records management staff assistance visits, information assurance office assessments, and inspector general assessments and inspections. Failure to comply the requirement will result in immediate removal of the information in question from its respective host system until the discrepancy is corrected. If the violation is deemed serious enough, the CSO has the authority to disconnect or shut down the system in question until the discrepancies are corrected.

8. All web pages should be in compliance with Department of Defense Web Site Administration Policies & Procedures, 25 Nov 98, at http://www.defenselink.mil/admin/dod web policy 12071998.html. Guidance and direction for Web pages are set forth on the Headquarters Air Force Communications Agency's (HQ AFCA, Scott AFB IL) Web site at: http:/www.afca.scott.af.mil/gc/gco/webstyle.

8.1.2. Organizations should be aware that the government domain may not provide adequate restriction for limited access pages. Many schools and public libraries have been found within this domain, due to the fact that their networks are acquired, installed and/or managed by state and local governments. Consider this when determining access requirements.

8.2.3. To clarify, this prohibition is for directories, not individual e-mail addresses and phone numbers, or even small blocks of office phone numbers. It should also be understood that the Privacy Act does not apply to government e-mail addresses and phone numbers; they are government owned and are within the public domain.

10.1. Any unauthorized or nonaccredited system discovered will be immediately disconnected until the system has been accredited and authorized for use by the DAA. This requirement will be an interest item on MAJCOM information assurance assessments.

10.3. (Added) Contractor-provided Web Server Support. Web servers hosting official government information must reside on a government-owned, government-controlled network. Official web sites and bulletin boards maintained on a contractor's site, using the contractor's network and resources are prohibited. Organizations may, however, commission contractor support on government-furnished equipment at a government site. Contractors providing such support are still subject to all provisions within this instruction.

Table 1. Line 5. (Added) Privacy Act Information. Minimum Access/Security Control- Password and ID/Encrypted.

Table 1. Note 3. (Added) Transmitting national security information (see paragraph 7.4.9 of this supplement) subject to provisions of Public Law 100-235, The Computer Security Act of 1987 (as amended),

across the nonsecure internet is prohibited unless it uses an encryption technology approved by the NSA. (NOTE: As of this writing, no such encryption technology has yet been approved by NSA.)

12. Data on a web server should be arranged in a hierarchical manner. The server's home page should reference the major categories of information maintained within the web server. Try to limit these major categories to no more than seven. The page must include the standard disclaimer/security banner and the name, e-mail, and phone of the webmaster or POC. As a minimum, the following categories are recommended for the web server's home page:

- Background/Mission. Pointer to mission statement or background information provided by an organization such as Public Affairs or the organization's History Office.
- Organizations or Org Chart. Pointer to page(s) of the organization and next-level subordinate activities.
- Search. Pointer to page(s) where full-text ,search and retrieval of information is provided.
- What's New. Pointer to page(s) indicating recently added or updated information on the server.
- Library. Pointer to area for accessing such things as publications, local and command internet policies, webmaster information, biographies, fact sheets, etc.

Pointers can be added as needed; however, it is imperative web server home pages contain only generic pointers to very abstract or "macrolevel" subject areas to facilitate the lowest common denominator--the new visitor who knows nothing about the site or the organization. A good benchmark for developing macrolevel pointers are "what's inside" sections of newspapers, usually located on the first page.

17. SBU information must be encrypted during transmission. Public Law 100-235, The Computer Security Act of 1987 (as amended), establishes the requirement for encryption of national security information. The Act does not distinguish protocols. For example, E-mail's Simple Mail Transfer Protocol (SMTP) is not viewed independently from the web's Hypertext Transfer Protocol (HTTP) or the internet's File Transfer Protocol (FTP).

Attachment 2

CHECKLIST FOR PREPARING MATERIAL FOR PUBLIC-RELEASE ON WWW

A2.1. No list can be all-inclusive in preparing material for the internet, but the following items must be considered. If you cannot answer "yes" to these questions, the material should not be released and should be reworked to fit the criteria, be posted on a limited access site if possible, or not be posted at all.

A2.1.1. Checklist to meet criteria from AFI 33-129, Transmission of Information via the Internet:

A2.1.1.1. Must be in compliance with DoD Guidance. (Web Site Administration Policies & Procedures, November 25, 1998; http://www.defenselink.mil/admin/dod_web_policy_12071998.html)

A2.1.1.2. Is the material of value to the general public? Do not place information that has value to only military or other government agencies on internet pages with unlimited access. (AFI 33-129, *Transmission of Information via the Internet*, para 7.2.1.2)

A2.1.1.3. Is the material free of classified information? (AFI 31-401, *Managing the Information Security Program)*

A2.1.1.4. Is the material free of Privacy Act-protected information? (AFI 37-132, *Air Force Privacy Act Program)*

A2.1.1.5. Is the material free of For Official Use Only (FOUO) information? FOUO is a marking placed on material to identify contents which are exempt from public release under the Freedom of Information Act (FOIA). Only material which qualifies under FOIA exemptions two through nine can be marked "FOUO." (AFI 37-131, *Freedom of Information Act Program)*

A2.1.1.6. Is the material free of FOIA exempt information for which the agency declines to make a discretionary disclosure? To ensure of this, the material should be compared against the nine FOIA exemptions. (AFI 37-131)

A2.1.1.7. Is the material free of DoD contractor proprietary information? (AFI 61-204, *Disseminating Scientific and Technical Information)*

A2.1.1.8. Does the material meet the requirements for releasing unclassified STINFO information (free of export-controlled information)? (AFI 61-204)

A2.1.1.9. Is the material free of unclassified information requiring special handling? (AFI 33-113, *Managing Messaging and Data Processing Centers*)

A2.1.1.10. Is the material free of critical information as outlined in AFI 10-1101, *Operations Security?* This includes sensitive mission data that by itself is unclassified, but when combined with other available data, may reveal classified information.

A2.1.1.11. Is the material free of phone number and electronic address directories? Publishing such directories is prohibited, because it invites mass mailing by commercial agencies and exposes organizations to attempts to overwhelm local networks. Keep in mind, this does not exclude ALL e-mail and phone numbers; some are required on web pages, and posting general numbers and small blocks of office numbers on lower level pages is encouraged. (AFI 33-129, para 8.2.3, as supplemented).

A2.1.1.12. Is the material free of commercial advertising and product endorsement, and free of graphics and artwork which may be proprietary or copyrighted? (AFI 33-129, paras 8.2.4 and 8.2.5)

A2.1.1.13. Is the material a professional representation of your organization and that of the Air Force?

A2.1.1.14. Is the material timely, current and accurate?

A2.2. If any material meets the following criteria, it may require clearance through the Air Staff or DoD level:

A2.2.1. Is or has the material potential to become an item of national interest or does it have policy implications?

A2.2.2. Does the material concern subjects of potential controversy among DoD components or with other Federal agencies?

A2.2.3. Does the material concern new weapons, weapon systems, or significant modifications or improvement to existing weapons, or systems, equipment, or techniques?

A2.2.4. Does the material concern military operations, operations security, potential operations and significant exercises?

A2.2.5. Does the material concern national command authorities and command posts?

A2.2.6. Does the material concern military applications in space, nuclear weapons, including weapon-effects research, chemical warfare, defensive biological and toxin research, high-energy lasers or particle beam technology?

A2.2.7. Does it concern materiel, including that submitted by defense contractors, involving militarily critical technology?

A2.2.8. Does the material concern communications security, signals intelligence and computer security?

A2.3. Primary guidance for releasing information to the public is found in AFI 35-205, *Air Force Security and Policy Review Program.*

DEBRA L. HALEY
Director of Communications and Information